

Coronavirus (COVID-19)

What companies must consider with regards to data protection



For additional information with respect to this Alert, please contact the following:

Charalambos Prountzos
Partner | Central, Eastern and Southeastern Europe & Central Asia (CESA) Law Leader | Head of Law & Funds Services
Phone: +357 22669699
E-mail: Charalambos.Prountzos@cylaw.ey.com

Iacovos Kouppas
Senior Manager
Legal Services - Head of Corporate and Digital Law services
Phone: +357 22669699
E-mail: Iacovos.Kouppas1@cylaw.ey.com

Executive summary

In light of the COVID-19 outbreak employers have had to adopt a number of measures for the purpose of preventing and/or containing COVID-19 while having to adjust their work procedures to the new realities we are currently facing. Such measures and procedures may involve extensive collection and processing of personal data, especially health data. To this end, ensuring that all new and/or modified procedures are in line with the data protection regime constitute an integral part in both corporate and state responses.

With the spread of COVID-19 companies have been forced to engage in an extensive collection and processing of personal data for the purpose of protecting their employees and clients. The foregoing measures involve processing of personal data including special categories of sensitive personal data, like travel-reporting information, health data (such as health examinations and reporting of symptoms) and tracing of personal contacts. Such data may be collected either via questionnaires, health checks and personal feedback whilst they may relate to employees or contractors and their relatives as well as visitors and/or clients.

Furthermore, compliance with governmental measures and new local legislative measures could also force companies to adopt new procedures in order to be in a position to comply with their newly enforced obligations. Finally, the new working environment adopted by a lot of companies, such as the "work-from-home" policies, could also mean that new procedures are required with regards to the processing of personal data of employees and clients.

Detailed discussion

GDPR is a broad piece of legislation and provides for rules that also apply to the processing of personal data in a context such as the one relating to COVID-19. The GDPR allows competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein.

With regard to the processing of personal data, including special categories of data by competent public authorities (e.g. public health authorities), Articles 6 and 9 of the GDPR enable the processing of personal data, in particular when it falls under the legal mandate of the public authority provided by national legislation and the conditions enshrined in the GDPR.

In the employment context, the processing of personal data may be necessary for compliance with a legal obligation to which the employer is subject to, such as obligations relating to health and safety in the workplace, or for the public interest, such as the control of diseases and other threats to public health. The GDPR also foresees derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for reasons of substantial public interest in the area of public health (Art. 9.2.i), on the basis of Union or national law, or where there is the need to protect the vital interests of the data subject (Art.9.2.c), as recital 46 explicitly refers to the control of an epidemic.

CORE PRINCIPLES

Personal data that is necessary to attain the objectives pursued should be processed for specified and explicit purposes. Ensuring the health and safety of employees could constitute lawful processing in line with Article 6 of the GDPR. Employers may lawfully process personal data, if such processing is necessary in order to protect the vital interests of their personnel and relatives. An interest is deemed to be vital only when it is essential for the life of the data subject or that of another natural person. The monitoring of epidemics is a type of processing, which may serve both important grounds of public interest and the vital interests of data subjects (as per recital 46 of the GDPR).

It is important that the employer takes all necessary action to safeguard the secure and lawful processing of any personal data for the above purposes. Thus, it is imperative that the data subjects receive transparent information on the processing activities that are being carried out and their main features, including the retention period for collected data and the purposes of the processing. The information provided should be easily accessible and provided in clear and plain language.

Furthermore, it is important to adopt adequate security measures and confidentiality policies ensuring that personal data are not disclosed to unauthorised parties. Measures implemented to manage the current emergency and the underlying decision-making process should be appropriately documented.

Finally, employers must take into account the proportionality principle. The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved. Invasive measures, such as the “tracking” of individuals (i.e. processing of historical non-anonymised location data) could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing. However, it should be subject to enhanced scrutiny and safeguards to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation). Thus, it is important that all necessary actions, notifications, documents and procedures are taken and followed by the employers with regards to the processing of personal data they are about to engage.

COVID - 19 - The most important facts and questions

- ▶ **Can an employer require visitors or employees to provide specific health information in the context of COVID-19?**

The application of the principle of proportionality and data minimisation is particularly relevant here. The employer should only require health information to the extent that national law allows it. Where necessary and provided all proper actions and notifications have been taken, the employer may proceed with processing that would be necessary to protect the vital interests of their personnel by deterring or delimiting exposure of their employees to COVID-19. However, in all cases, processing must only take place when it can be manifestly based on a legal basis as per the GDPR.

In all cases, employers are required to comply with the general principles of processing enlisted in article 5 of the GDPR, the principles of data minimization and storage limitation being of particular importance under these circumstances.

▶ **Is an employer allowed to perform medical check-ups on employees and process their health data?**

In principle, employers should only perform medical checks and access and process health data if their own legal obligations require it. As a general rule, employers may lawfully process special categories of personal data of their employees only if processing is necessary for the assessment of the working capacity of an employee under the responsibility of a professional subject to the obligations of professional secrecy (as per Article 9 of the GDPR). Such processing should be restricted to specific cases, i.e. where there is strong suspicion of infection and may only be conducted by a professional physician or healthcare professional.

Thus, general blanket measures of health data processing across all employees, contractors and visitors are not advisable and would be hard to accommodate under this legal basis.

▶ **Can an employer disclose that an employee is infected with COVID-19 to his colleagues or to externals?**

Employers should inform staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary. In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g. in a preventive context) and where the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected.

▶ **What information processed in the context of COVID-19 can be obtained by the employers?**

Employers may obtain personal information to fulfil their duties and to organise the work in line with national legislation. Employers may adopt health and safety procedures that would lawfully impose reporting obligations to employees in respect of suspected cases of infection by COVID-19 and lawfully collect such information under article 9.2.i. of the GDPR.

▶ **What kind of security measures should companies have in place for homeworking during this period?**

If employees process personal data from home, it is important to provide them with the company's internal technical and organizational

measures (TOMs) and ensure that they comply with them at all times. For example, documents containing personal data must be kept confidential, i.e. out of reach of spouses, children or visitors. It is the duty of every company to publish and inform its employees accordingly and to oblige them to comply with TOMs. Furthermore, companies should ensure that homeworking does not violate any contractual obligations with third parties.

Compliance check-list

- Engage your Data Protection Officer in the procedure
- Keep up to date with the guidelines and measures taken by both local and European authorities
- Provide the necessary information to the data subjects involved in any new and/or updated processing activities
- Respect data subjects' rights throughout this difficult process
- Put in place appropriate corporate policies and procedures
- Maintain the necessary and appropriate internal documentation on the lawful bases of any protective measures adopted
- Conduct Data Protection Impact Assessments (DPIA)
- Maintain all necessary measures for data security and confidentiality.
- Update your data protection documentation, in particular the data protection impact assessment (DPIA) and the register of processing activities.

How can you best prepare and respond to the COVID-19 crisis?

- Information - obtain and provide all necessary information on a regular and transparent basis
- It is true that the risks and dangers posed by COVID-19 may justify normally unlawful data processing activities as long as they protect the health of others. However, there are legal limits and technical and organizational measures (TOMs) to be observed under data protection law.
- Be vigilant and alert to changes in standard processes. In general, every deviation requires an assessment under data protection law.

The data of your employees is a valuable asset that must be protected. In this respect, precautions should be taken to ensure that your company can master the data protection and IT law challenges of the COVID-19 with confidence.

How EY Cyprus can assist

Our specialised GDPR and employment law team is ready to discuss with you and assist you with:

- How data protection requirements for the processing of highly sensitive personal data (health data) can be implemented in your company in individual cases.
- How to update and adapt your processes due to COVID-19 and updating all data protection documentation, i.e. data protection impact assessment (DPIA), the register of processing activities etc.
- How to prepare all important instructions for your employees, any data protection declarations as well as data protection documentation with regard to COVID-19.
- Conducting or updating data protection impact assessments (DPIA).
- Possible procedures initiated by the authorities in terms of data protection.
- Adapting processes to the COVID-19 risks in accordance with data protection regulations.
- Analyzing data protection agreements with third parties regarding the data protection permissibility of homeworking.
- Measures and/or procedures to be implemented to facilitate homeworking by employees without breaching any data protection regulations.

EY | Assurance | Tax | Transactions | Advisory
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com

© 2020 Ernst & Young Cyprus Ltd
All rights reserved.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

ey.com/cy